



# FOIP FOLIO

## THE OIPC CELEBRATES ITS 5th ANNIVERSARY

The Office of the Information and Privacy Commissioner (OIPC) with a full time Commissioner was launched 5 years ago on November 1, 2003. Hopefully you will have seen positive changes in our provincial FOIP regime since that time. The goals of the office have been outlined in successive business plans for the OIPC available on our website, [www.oipc.sk.ca](http://www.oipc.sk.ca) under the *Annual Reports* tab. These business plans have included specific performance measures for each of the last 4 fiscal years. Our Annual Reports, also available on the website, provide more detailed information on what has been achieved by the office over the past half decade. Commissioner Gary Dickson recently praised the dedication and diligence of the men and women that have worked in the OIPC over the last five years. "We were fortunate to have had the benefit of very talented individuals with a wonderful work ethic who have laid the foundation for our fledgling OIPC." In addition, since the FOIP regime is much more than our office, credit goes to FOIP Coordinators throughout Saskatchewan who have

enhanced, in their public bodies, compliance with FOIP, LA FOIP, and HIPA. Credit is due Justice Deputy Minister, **Doug Moen**, for the creation of the Access and Privacy Branch and ongoing support for the important work of that branch. In

terms of health information, much progress has been made by Saskatchewan Health and regional health authorities. Congratulations to **Jacque Messer-Lepage**, her predecessors and her current team in the Health ministry for that achievement. We are grateful for the support from the public for our work and the patience and understanding afforded us as we have slowly increased our capacity while dealing with a rapidly increasing case load. Finally, our office has received essential support from the

current and former Speaker and members of the Legislative Assembly since 2003. We look forward to the next five years and the further progress that we can collectively achieve in ensuring that the residents of Saskatchewan enjoy the full measure of their statutory access and privacy rights!



## TABLE OF CONTENTS

|   |   |   |   |
|---|---|---|---|
| The OIPC Celebrates its 5th Anniversary .....   | 1 | Social Networking Sites, Read the Fine Print .....              | 4 |
| <i>Privacy Perspectives From the Privacy Commissioner of Canada</i> .....                                   | 2 | Identity Fraud: No Really, It Wasn't Me .....                   | 5 |
| Prairie Health Information Privacy Day 2008 .....   | 2 | B.C. Supreme Court Awards Damages for Invasion of Privacy ..... | 6 |
| New Practice Tool for Exercising Discretion to Disclose Personal (Health) Information Without Consent ..... | 2 | Pakistan Poised to Enact Freedom of Information Law. .          | 6 |
|   |   | Future Events .....   | 7 |



---

## PRIVACY PERSPECTIVES FROM THE PRIVACY COMMISSIONER OF CANADA

The Office of the Privacy Commissioner of Canada (PCC) has published the first edition, Fall 2008 (Issue 1), of its new e-newsletter *Privacy Perspectives*. It is available on the OPC website: [http://www.privcom.gc.ca/newsletter-bulletin/fall2008/index\\_e.asp](http://www.privcom.gc.ca/newsletter-bulletin/fall2008/index_e.asp).

Published four times per year, every issue will contain information about how the PCC is working to protect and promote privacy rights. The e-newsletter also includes links to the

office's publications and tools and offers real-world examples of how federal privacy legislation comes into play by highlighting the office's most recently published case summaries.

Just as with our e-newsletter, readers have the option of subscribing online to receive issues via e-mail.

---

## PRAIRIE HEALTH INFORMATION PRIVACY DAY 2008



If you did not have opportunity to attend this Winnipeg conference, you nonetheless can still reap some of the benefits.

Presentations given by speakers at the above conference hosted by the offices of Alberta and

Saskatchewan's Information and Privacy Commissioners and the Manitoba Ombudsman's Office on October 22, 2008 are now available for viewing or downloading at <http://verney.ca/hipd2008/presentations.php>.

---

## NEW PRACTICE TOOL FOR EXERCISING DISCRETION TO DISCLOSE PERSONAL (HEALTH) INFORMATION WITHOUT CONSENT

**Ann Cavoukian**, Ontario's Information and Privacy Commissioner, and **David Loukidelis**, Information and Privacy Commissioner of British Columbia, recently devised a tool to help public bodies decide when to disclose personal information without the consent of the subject individual. The tool can be found on the Ontario IPC website ([http://www.ipc.on.ca/images/Resources/ipc-bc-disclosure-edu\\_826594762500.pdf](http://www.ipc.on.ca/images/Resources/ipc-bc-disclosure-edu_826594762500.pdf)) and on the B.C. OIPC website (<http://www.oipc.bc.ca/pdfs/Policy/ipc-bc-disclosure-edu.pdf>).

The new tool describes a variety of scenarios that a public body might face, and delineates the steps

that can be taken to deal with them. For example, if an individual poses a compelling risk to the safety of himself (e.g., suicide), to others (e.g., homicide) or to the public interest (e.g., a bombing or school shooting), there are provisions in B.C.'s and Ontario's privacy laws that allow for the disclosure of personal (health) information in order to mitigate that risk. In a nutshell, the tool emphasizes that **life trumps privacy**.

*Continued on Page 3 (New Practice Tool)*



## NEW PRACTICE TOOL (CONTINUED)

Similar to B.C.'s legislation, Saskatchewan's *The Freedom of Information and Protection of Privacy Act* (FOIP) and its counterpart for local authorities (LA FOIP) allow public bodies to disclose personal information without consent in order to "protect the mental or physical health or safety of any individual" [FOIP section 29(2)(m) and LA FOIP section 28(2)(l)]. Likewise, Saskatchewan's *The Health Information Protection Act* (HIPA) allows trustees to disclose personal health information without consent where there are reasonable grounds to believe "that the disclosure will avoid or minimize a danger to the health or safety of any person" [HIPA section 27(4)(a)].

In addition to reminding public bodies that there are legitimate grounds for disclosing personal information without consent in specific circumstances, the tool emphasizes the need for specific policies and well-rehearsed procedures for making difficult and often very time-sensitive decisions. For example, staff should be well-trained in the nuances of the applicable privacy laws, and clear decision-making strategies should be delineated (who makes them, using what criteria, etc.). Furthermore, emergency contact methods should be determined in advance so that if a decision is made to disclose, it can be done immediately and efficiently. Finally, the tool discusses the need to notify individuals and the public both of the potential for personal information to be disclosed without consent in cases where safety is at serious risk, and retroactively, if/when such a disclosure has been made.

It is important to note that the exercise of discretion in cases of minimizing danger to health

or safety should be made with due consideration, and the burden of proof is on the public body or trustee to justify the disclosure. A helpful general test is as follows:

1. There must be a clear and present risk of significant harm.
2. Release of the information must be likely to reduce the risk.
3. There must be no less intrusive way to reduce the risk of harm.

Please also note that while the decision to disclose under such circumstances is *discretionary* under HIPA, FOIP and LA FOIP, your own professional codes of conduct and other applicable laws may make disclosure in such circumstances *mandatory*. For example, under *The Gunshot and Stab Wounds Mandatory Reporting Act* disclosing specific personal health information to the police is required in prescribed circumstances.

**CAUTION:** When reviewing the B.C. and Ontario materials, please note that both of those provinces<sup>1</sup> have a 'public interest override' in their FOIP laws. Such an override creates a positive (mandatory) duty for the head of a public body to disclose information in certain circumstances. This is usually where there is a risk of serious injury to the health or safety of the public or where there is a risk of significant harm to the environment. FOIP in Saskatchewan does not include this feature. Nonetheless, the head in this province still has a discretion to disclose to avoid injury.

<sup>1</sup> The public interest override is also found in FOIP laws in Newfoundland and Labrador, Prince Edward Island and Alberta.



## SOCIAL NETWORKING SITES, READ THE FINE PRINT

Social networking sites, such as Facebook, have received significant criticism from individuals and organizations concerned with the impact of these sites on the privacy of users. Much of the criticism relates to how information is collected, used, and disclosed by these websites. Proponents of social networking sites argue that users voluntarily agree to use these sites, and share only that information about themselves that they wish to disclose. To some degree this is true, but in reality the privacy policies and terms of use agreements (TUA) of many of these sites weaken such arguments.

Frequently TUAs and privacy policies are written in overly legalistic language, and are so lengthy that people will only read part of them if they read them at all. The following excerpts from Facebook's TUA and privacy policy illustrate why it is so important to carefully read these documents before using the site.

This excerpt is from Facebook's TUA (available at <http://www.facebook.com/terms.php>)

By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. You may remove your User Content from the Site at any time. If you

choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.

This excerpt is taken from Facebook's privacy policy (available at <http://www.facebook.com/policy.php>)

We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities.

We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile.

If you are currently using a social networking site, or are thinking of joining one, we strongly recommend that you carefully read both the TUA and the privacy policy of the site before reaching a decision on your use of the site.







## IDENTITY FRAUD: NO REALLY, IT WASN'T ME



In an article, *It Could Happen To You*, in the March 2006 issue of this newsletter, we offered results of a national survey of victims of identity theft in Canada. We defined identity theft as "the use of someone else's personal information,

without his or her knowledge or consent, to commit a crime, such as fraud, theft, or forgery."

What is the difference between identity theft and identity fraud? Though the term *identity theft* is commonly used to mean *identity fraud*, there is no universally accepted definition for either. For a comprehensive listing of definitions, we draw your attention to The Canadian Internet Privacy and Public Interest Clinic's (CIPPIC) paper *Identity Theft Introduction and Background*.<sup>2</sup> Though hard to distinguish, identity theft generally results when another uses your personal information to impersonate you and, for example, applies for new credit in your name. Identity fraud, on the other hand, occurs when an unauthorized person uses your account information (e.g., credit card number) in order to make unauthorized financial transactions, without any additional attempts to impersonate you. Nonetheless, both involve someone else using your personal information/personal health information without your knowledge or consent for their benefit at your expense, literally as reported in a recent article.<sup>3</sup> A new national survey conducted in February by researchers at the McMaster eBusiness Research Centre in

Hamilton, reveals that over the past year nearly 1.7 million Canadian consumers were victims of identity fraud and that, while attempting to resolve the fraud, they spent approximately 20 million hours and are out of pocket more than \$150 million.

In yet another article on the same topic, it was reported that the majority of the cases identified in the survey involved debit card skimming, with the rest involving identity theft or impersonations used to set up new accounts, lines of credit, mortgages, or government benefits.<sup>4</sup> It was noted that most of the victims had no idea how they were targeted, but "it turns out old-fashioned shopping is riskier than online commerce; 25 per cent of cases were associated with business transactions conducted in person compared to 15 per cent linked to online transactions. Debit card skimming operations made up another 13 per cent of the cases."<sup>5</sup>

Some basic ways you can protect yourself include shredding financial documents, avoiding giving your credit card information to service industry workers that take it out of sight to swipe, regularly requesting a copy of your credit report, and consider limiting the amount of shopping you do on line.

<sup>2</sup> Available online: <http://www.cippic.ca/documents/bulletins/Introduction.pdf>.

<sup>3</sup> newsBlaze (Folsom, CA), 1.7 Million Canadians Victims of ID Fraud. November 17, 2008 <http://newsblaze.com>.

<sup>4</sup> CWN via The Gazette (Montreal), Identity theft plagues 1.7M Canadians. November 17, 2008 <http://www.montrealgazette.com/>.

<sup>5</sup> Sarah Schmidt, Canwest News Service, Identity theft victims total 1.7 million: survey. Published: Tuesday, November 18, 2008.



---

## B.C. SUPREME COURT AWARDS DAMAGES FOR INVASION OF PRIVACY



Earlier this fall, a Vancouver judge awarded a tenant damages arising from the landlord's installation of video surveillance equipment. The equipment was installed in a hallway but permitted very close-up and detailed images of anyone entering and exiting the tenant's suite. This award was made under the B.C. *Privacy Act*

that is very similar to the Saskatchewan *Privacy Act*. This statute is available at our website, [www.oipc.sk.ca](http://www.oipc.sk.ca) under the *Legislation* tab. The decision is Heckert v. 5470 Investments Ltd. [2008] B.C.J. No. 1854.

---

## PAKISTAN POISED TO ENACT FREEDOM OF INFORMATION LAW



Pakistan, influenced by the success of India's Freedom of Information law, has produced a draft *Freedom of Information Bill, 2005*. Similar legislation is being drafted by Nepal and Bangladesh, also modelled on the India law. One important improvement in the Pakistan draft bill was noted by the Centre for Peace and Development Initiatives in India. This was the inclusion of whistleblower protection. Activists in India have reported instances of the government harassing access requesters. Prominent activist, **Aruna Roy**, a woman who

has come to Canada several times to speak at access conferences, is reported in the *Hindustan Times* (Nov. 11, 2008, p. 11) to have said: "fear of exposure of wrongdoings makes government officials hostile towards information seekers." The Pakistan draft bill gives the office of the ombudsman-the final authority in implementation of the law- the power to ask the government to provide protection to information seekers. There is nothing equivalent in the Indian legislation.



## **FUTURE EVENTS**

**January 19-20, 2009 - Privacy Compliance Conference 2009 – Calgary, AB**  
(visit <https://www.canadianinstitute.com/Home.htm> for more details)

**February 3, 2009 - 10th Annual Privacy and Security Conference – Victoria, BC**  
(visit <http://www.rebootconference.com/privacy2009/> for more details)

**February 9, 2009 - CBA Privacy & Access Law South Section Meeting - Topic: "Identity Theft" - Regina, Saskatchewan, Hotel Saskatchewan at 12:00 pm (to register call the CBA at 306-244-3898)**

**February 10, 2009 - CBA Privacy & Access Law North Section Meeting - Topic: "Identity Theft" - Saskatoon, Saskatchewan, Saskatoon Club at 12:00 pm (to register call the CBA at 306-244-3898)**

**March 10, 2009 - CBA Privacy & Access Law South Section Meeting - Topic: "Electronic Health Records" - Regina, Saskatchewan, Hotel Saskatchewan at 12:00 pm (to register call the CBA at 306-244-3898)**

**March 9, 2009 - CBA Privacy & Access Law North Section Meeting - Topic: "Electronic Health Records" - Saskatoon, Saskatchewan, Saskatoon Club at 12:00 pm (to register call the CBA at 306-244-3898)**

**April 4-8, 2009 - HIMSS09 Annual Conference and Exhibition – Chicago, Illinois**  
(visit <http://www.himssconference.org/docs/HIMSS09MINIbrochure.pdf> for more details)

**May 31-June 3, 2009 - e-Health 2009: Leadership in Action – Quebec City, Quebec**  
(visit <http://www.e-healthconference.com/> for more details)

### **OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER**

**503 – 1801 Hamilton Street  
Regina, Saskatchewan  
S4P 4B4**

**Telephone: (306) 787-8350 / Toll Free: 1-877-748-2298**

**Fax: (306) 798-1603**

**E-mail: [webmaster@oipc.sk.ca](mailto:webmaster@oipc.sk.ca)**

**Website: [www.oipc.sk.ca](http://www.oipc.sk.ca)**

*If you wish to subscribe to the Saskatchewan FOIP FOLIO, please  
send your e-mail address to [webmaster@oipc.sk.ca](mailto:webmaster@oipc.sk.ca).*